



AFRL-RX-WP-TR-2014-0166

EVALUATING SECURITY TECHNOLOGIES USED TO ENHANCE PHYSICAL SECURITY CAPABILITIES AT DOMESTIC AND DEPLOYED BASES

**Thomas R. Monaco
Applied Research Associates, Inc.**

**JULY 2013
Final Report**

Distribution A. Approved for public release; distribution unlimited.

See additional restrictions described on inside pages

STINFO COPY

**AIR FORCE RESEARCH LABORATORY
MATERIALS AND MANUFACTURING DIRECTORATE
WRIGHT-PATTERSON AIR FORCE BASE, OH 45433-7750
AIR FORCE MATERIEL COMMAND
UNITED STATES AIR FORCE**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the USAF 88th Air Base Wing (88 ABW) Public Affairs Office (PAO) and is available to the general public, including foreign nationals.

AFRL-RX-WP-TR-2014-0166 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

//Signature//
ANDREW T. JEFFERS, Contract Monitor
For: Walter Waltz
Airbase Technologies Division
Air Force Research Laboratory

//Signature//
PAMELA M. SCHAEFFER, Acting Chief
Integration and Operations Division
Materials and Manufacturing Directorate
Air Force Research Laboratory

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) July 2013		2. REPORT TYPE Final		3. DATES COVERED (From – To) 22 July 2009 – 30 June 2013	
4. TITLE AND SUBTITLE EVALUATING SECURITY TECHNOLOGIES USED TO ENHANCE PHYSICAL SECURITY CAPABILITIES AT DOMESTIC AND DEPLOYED BASES				5a. CONTRACT NUMBER FA4819-09-C-0011	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER 0999999F	
6. AUTHOR(S) Thomas R. Monaco				5d. PROJECT NUMBER GOVT	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER X0BA	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Applied Research Associates, Inc. 1235 S. Clark Street, Suite 1212 Arlington VA 22202				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory Materials and Manufacturing Directorate Wright Patterson Air Force Base, OH 45433-7750 Air Force Materiel Command United States Air Force				10. SPONSOR/MONITOR'S ACRONYM(S) AFRL/RXQ	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) AFRL-RX-WP-TR-2014-0166	
12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution A. Approved for public release; distribution unlimited. This report contains color.					
13. SUPPLEMENTARY NOTES PA Case Number: 88ABW-2012-2144; Clearance Date: 12 April 2012.					
14. ABSTRACT This preliminary report focuses on the support and analysis provided to the Air Force Research Laboratory, Airbase Technologies Division in the area of advanced capabilities and technologies that facilitate contingency base operations, combat support functions, to include life-cycle support and supply chain management, and force protection in homeland security and Air Expeditionary Forces operations.					
15. SUBJECT TERMS secure wireless communications, behavioral analysis, and installation access control					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 16	19a. NAME OF RESPONSIBLE PERSON (Monitor) Andrew T. Jeffers
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUBER (include area code) (937) 904-4011

1. SUMMARY

This draft final report focuses on the work performed under this contract over the course of 4 years providing analysis, research and development (R&D) for the Air Force Research Laboratory's (AFRL), Airbase Technologies Division (RXQ).

Work performed included areas primarily in support of force protection and physical security with a focus on:

- Secure Wireless Communications
- Installation Access Control
- Integrated Waterside Security
- Behavioral Analysis, and
- Other areas as prescribed by the AFRL customer or associated Government Leads

This report will provide a brief history of each of the areas described above, work performed and the resultant recommendations/solutions provided for each area.

2. INTRODUCTION

2.1. Purpose

The purpose of this project was to research several business/functional areas that require analysis for the DoD and other Agencies to provide the best possible solutions to complex problems in the area of Force Protection and Physical Security for personnel, installations, equipment and both nuclear and non-nuclear (conventional) weapon systems. Research and analysis is necessary for not only technology and acquisition approaches, but for concepts of operations, requirements analysis and industrial base life cycle support. There are many sub systems of Force Protection and Physical Security that create the holistic “system of systems” approach to effective results not to mention the integration that is required to have seamless solutions.

2.2. Background

Over the past 4 years, ARA was asked to support AFRL/RXQ and other Service/Agencies in the required research and development of key areas and technologies in very specific force protection missions. These areas were:

- Secure Wireless Communications
- Installation Access Control
- Situational Awareness
- Behavioral Analysis
- Integrated Waterside Security, and
- Other areas as prescribed by the AFRL customer or associated Government Leads

What follows will be a summary of each of the areas outlined with the result of the work done for and on behalf of the DoD and AFRL/RXQ.

3. SECURE WIRELESS COMMUNICATIONS

BACKGROUND

At the June 2007 Nuclear Weapons Security Summit, a member asked, “Where can we use wireless with physical security?” The Secure Wireless Communications Working Group (SWCWG) was chartered to study the challenge of using wireless communications with nuclear physical security systems and make assessments/recommendations for the path ahead.

Since FY08 the SWCWG has provided the nuclear physical security community a single point of focus for wireless communications issues relating to the use of wireless communications with nuclear physical security. The group provides a forum and facilitation for discussions related to wireless communications and executes taskings from the PSEAG to address relevant issues raised by the nuclear physical community. Results generated from the SWCWG are shared with the non-nuclear physical security community as many of them overlap with conventional physical security applications.

All deliverables associated with the Secure Wireless Communications Working Group project have been met and delivered.

SWCWG Program Execution FY08-10

FY08-09

A five year SWCWG Strategic Plan (**deliverable**) was developed in FY08 beginning with an equipment focused Wireless Communications Study (WCS) conducted by the Space and Naval Warfare Center, Atlantic. The study reviewed the status of current wireless communications issues for three specific DoD programs: remotely operated weapon systems (ROWS), remote visual assessment (RVA), and wireless perimeter intrusion detection systems (PIDS). The WCS identified three major findings; Wireless technology requirements were not fully developed or understood; Policy was missing or contradictory; and not all security applications are suitable for wireless communications use (e.g., wireless technologies are not robust enough for command and control of remotely operated weapon systems).

Results of the FY08 WCS were presented to the SWCWG. Based on the results, the SWCWG recommended to the August 2008 Nuclear Security Summit a way ahead for FY09. The way ahead included a requirements analysis review of the DoD Nuclear Security Roadmap and similar DOE mission areas that are using or considering the use of wireless communications with nuclear physical security systems (PSS), and an ad-hoc task to investigate service approaches to Situational Awareness (SA). The SA task addressed the operational, policy, security, and technical requirements for the transmission, display and storage of PSS information used in the protection of nuclear assets. The information displayed is commonly referred to as, “Situational Awareness (SA)” and/or “Common Operating Picture (COP)” data.

FY09-10

The follow-on FY09 Requirements Analysis (**deliverable**) helped to further define the issues by focusing on the twelve DoD Nuclear Security Roadmap Mission Areas and three similar DOE environments. The review of these mission areas consisted of site visits to Minot Air Force Base, Kings Bay Naval Submarine Base, Sandia National Laboratory-Albuquerque, and Los Alamos National Laboratory to survey and interview Services and Agencies experimenting with or deploying wireless. Findings of the survey and interviews consisted of:

- All interviewee's stated policy is lagging technology preventing successful deployment.
- Policy requires updating to meet the application of wireless with nuclear physical security- define the "higher standard"
- Wireless is required (derived) based on services and agencies cost benefit analysis and desired ability to provide greater situational awareness
- Wireless technical vulnerabilities and mitigations are not fully understood for wireless applications
- Need to identify acceptable Information Assurance Defense in Depth and risk management strategies
- Who and what is the threat needs defining

Based on the findings the FY09 Requirements Analysis, the SWCWG recommended a Table Top Exercise (**deliverable**) to:

- Provide recommendations/improvements to Policy
- Work with NSA to establish acceptable wireless technical vulnerability mitigations
- Determine the cyber threat in relationship to the design basis threat/graded security protection (NSTCA)

The FY09-10 Situational Awareness Study (**deliverable**) conducted similar interviews and analysis and resulted in some overlapping findings, including:

- Identified inconsistencies on how services and agencies treat similar SA data (UNCLASSIFIED, UCNI, CONFIDENTIAL)
- Classification Guidance and policy are not well defined for situational awareness data in support of nuclear asset security.
- There is a lack of minimum essential standards in policy and classification guidance defining data classification during transmission, storage, and display.
- Clear guidance does not exist for the control of wireless solutions for use with nuclear physical security.

Recommendations from the Situational Awareness Study noted similarities in findings and recommendations from the previous studies and recommended a consolidated TTX approach including:

- Services should evaluate DOE NightOwl software for possible use in DoD Physical Security and SA architectures (potential leveraging and cost savings).
- Services and DoD Policy makers should evaluate adapting or adopting all or part of DOE TNP-26 for its definitive guidance on implementation of wireless solutions and treatment of SA data (opportunity).
- Consider Joint experimentation to demonstrate utility and interoperability of SA data approaches.
- Incorporate SA study Lessons Learned into the FY11 Secure Wireless Communications Working Group (SWCWG) Table Top Exercise (TTX) planning and execution (adopted by the SWCWG in March 2010).
- Recommended combining results of SA study into SWCWG TTX.

FY10-11

To bring the lessons learned from the prior studies into a single point of focus, the FY10-11 Table Top Exercise was conducted in December 2010. During the TTX, participants benefitted from the SWCWG WCS, Requirements Analysis, and Situational Awareness Study efforts identified above and in Figure 1 below.

FY08 Understand the problem	FY09 Identify Options	FY10 Recommend Solutions
Wireless Communications Study <ul style="list-style-type: none"> • SPAWAR—Equipment focused <ul style="list-style-type: none"> ○ PIDS, ROWS, RVA ○ Market research ○ ID wireless capabilities ○ Investigate system capabilities, performance requirements • Wireless requirements not well defined • Classification of data not well defined • Long term testing required • Build a Qualified Products List 	Requirements Analysis Study <ul style="list-style-type: none"> • SWCWG Sub Group conducted <ul style="list-style-type: none"> ○ Review wireless requirements of 12 DoD Nuclear Roadmap environments ○ Policy lacking ○ Need to understand/define Threat (Cyber vs NSTCA) ○ Wireless technical vulnerability mitigation ○ Encourage NSA involvement ○ Conduct Table Top Exercise to flesh out solution 	Situational Awareness Study <ul style="list-style-type: none"> • Classification of Data during transmission, display, and storage • Wired or wireless transmission of data doesn't change classification • Data classification guidance near non-existent or not understood • Combine SA study results into SWCWG TTX

Figure 1 SWCWG Study Areas

The four main **deliverables** from the FY10-11 TTX were to:

- Identify applicable policy and if necessary suggest changes to policy for wireless communications use with nuclear physical security systems

- o Policy recommendations were provided to NSA to create minimum standards necessary for the wireless transmission of sensitive but unclassified data to include DoD unclassified controlled nuclear information. NSA transmission to OASD of these first ever standards were due 31 March 2011.
- Recommend changes to SCG as it relates to using wireless communications,
 - o Classification guidance that was not in existence prior to this effort were created for the services to incorporate.
- Facilitate a wireless threat vulnerability assessment working group;
 - o With assistance from NSA and DIA a wireless vulnerabilities matrix was produced to address information assurance concerns against spoofing, masquerading, man in the middle attacks, authentication, and access for wireless use with nuclear physical security
- Analyze how the current Design Basis Threat/Graded Security Protection (DBT/GSP) is affected by the use of wireless communications (cyber threat);
 - o The cyber threat to wireless systems was not existent prior to this effort. With the assistance of DIA, a baseline cyber threat has been defined for nuclear physical security systems employing wireless.

4. INSTALLATION ACCESS CONTROL

4.1 Background

Current Department of Defense (DoD) installation access control procedures are governed and implemented under Component-unique direction and are not fully interoperable between Component installations. At present, no enterprise capability exists for equipping DoD installations with electronic authentication of credentials. The Office of the Under Secretary of Defense for Intelligence (OUSD(I)) **Directive-Type Memorandum (DTM) 09-012** (Appendix 1) mandates Physical Access Control Systems (PACS) must support a DoD-wide and federally interoperable access control capability that can authenticate United States Government (USG) physical access credentials and support access enrollment, authorization processes, and securely share information; with provisions for security forces and/or guards to conduct a physical and visual inspection of credentials until electronic PACS are fully deployed, where applicable. Additionally, **Section 1069 of Public Law 110-181** (Appendix 2), tasked the Secretary of Defense (SECDEF) to determine the –fitness‖ of personnel entering military installations in the United States.

4.2 Purpose and Goals

To move toward compliance with DTM 09-012, the DoD Physical Security Equipment Action Group (PSEAG) agreed to sponsor a series of Defense Installation Access Control (DIAC) Working Group (WG) Demonstrations. Demonstration I was conducted from 7-10 Jun 2010 at three locations: Site C-3/Eglin AFB, Florida (USAF), Space & Naval Warfare Systems Command (SPAWAR), Charleston, South Carolina (USMC) and the Washington Navy Yard, Washington, DC (USN). The focus of Demonstration I was to verify the ability of physical access control systems to exchange data with an authoritative source system, the Defense Enrollment Eligibility Reporting System (DEERS), to authenticate credentials via middleware/regional server within a web services architecture. In addition, it focused on the capability of web services to return information to PACS. Demonstration I validated that the capability currently exists to immediately exchange data with an authoritative source (DEERS) via a middleware/regional server within a web services architecture and to return information accurately to PACS. The demonstration was a success in that each of the Services' PACS was responsive and went to DEERS as the authoritative source without issue.

Demonstration II used four test sites, Site C3/Eglin AFB, FL (USAF); SPAWAR Charleston, SC (USMC), SPAWAR Lab San Diego, CA (Army) and the Washington Navy Yard, Washington, DC (Navy). The focus of this Demonstration was developing and evaluating a continuous information management capability to send information to the PACS when data on an individual's –fitness‖ for access to an installation changes. This capability was paired with an interoperability layer service (IoLS) that ensured the data reached each Service-level PACS so that the entry control point security guard will know whether to authorize or deny entry. The availability of National Crime Information Center (NCIC) and Terrorist Screening Database

(TSDB) data was demonstrated via a simulated database, accessed upon demand. Figure 2 diagrams the connectivity between the CIME, IoLS and the PACS.

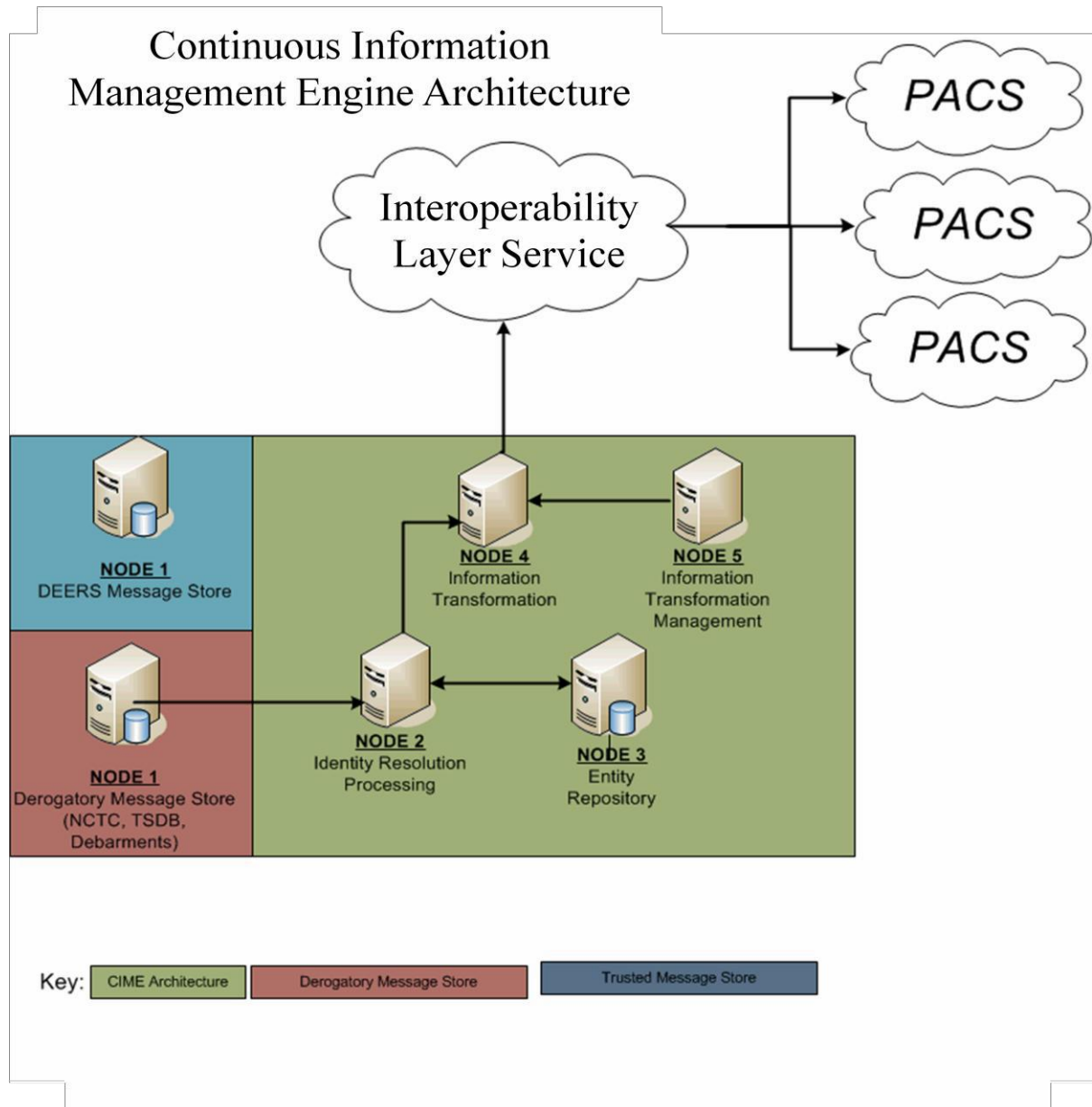


Figure 2 CIME/IoLS Architecture

4.3 Results and Findings

The results of Demonstration II proved the art-of-the-possible for delivering the ability to exchange personnel identification data between installation PACS, an Interoperability Layer Service (IoLS), a Continuous Information Management Engine (CIME) and test data representing authoritative source systems (NCIC & TSDB). Demonstration II also successfully

demonstrated the ability to pass registration, revocations, debarment, felony wants/warrants, and terrorist screening information between DoD Components. Unique to this Demonstration was the execution of Global Name Recognition, which is an enhanced name checking function that increases accuracy by matching across alternate forms of a given name. By creating a new Identity Management Enterprise Services Architecture and exercising it with a 100 percent success rate, the decision to proceed with the Architecture's continued evolution and future demonstration/implementations at operational DoD installations is fully supported.

5. BEHAVIORAL ANALYSIS

5.1 Problem

On November 5, 2009, tragedy struck when a gunman opened fire at the Soldier Readiness Center at Fort Hood, Texas. The individual was an officer in the Army, stationed at Fort Hood who had been granted the privileges of every vetted and credentialed Department of Defense (DoD) personnel who enter the gates of Fort Hood or any other DoD installation.

Following the shooting, then Defense Secretary Robert M. Gates established a task force to conduct the Department of Defense Independent Review Related to Fort Hood. In January 2010, the task force published the Independent Review, "Protecting the Force: Lessons from Fort Hood." The Fort Hood Independent Review contained 41 findings with subsequent recommendations to those findings.

Chapter 3 entitled, "Force Protection" contained nine findings. Finding 3.7 stated, "DoD installation access control systems and processes do not incorporate behavioral screening strategies and capabilities, and are not configured to detect an insider threat." Furthermore, the recommendations for the finding go on to say:

- Review best practices, including programs outside the U.S. Government (USG), to determine whether elements of those programs could be adopted to augment access control protocols to detect persons who pose a threat.
- Review leading edge tools and technologies that augment physical inspection for protecting the force.

On that day, the "insider threat" once again became front page news worldwide; only this time much like the aftermath of the Virginia Polytechnic Institute & State University's (Virginia Tech) shootings, a significant movement towards prevention and change was initiated.

5.2 Response

The Defense Installation Access Control (DIAC) Working Group under the leadership of the Physical Security Enterprise and Analysis Group (PSEAG) conducted a short term (6-month) research Study to address Finding 3.7. The Behavioral Analysis Study (herein otherwise referred to as the "research Study") was published in January 2011, after interviewing 38 individuals representing organizations across the USG, Academia, and Subject Matter Experts (SMEs).

In August 2011, the DIAC Working Group formed a Behavioral Analysis/Insider Threat (BA/IT) team and embarked on attacking the first recommendation from the research Study. The BA/IT team was instructed to conduct a Table Top Exercise (TTX) to assist the Services with developing and refining their requirements related to behavioral detection and the insider threat for the Force Protection/Physical Security community.

Between August 2011 and March 2012, the BA/IT TTX team interviewed and/or met with 65 individuals, expanding upon the list from the research Study. These interviews/meetings became more of a fact finding/discovery mission and laid the ground work for the formation and execution of the TTX. The team collected information in many areas which became the focal points of the TTX:

- Office of the Secretary of Defense (OSD) and Service Insider Threat Working Groups
- Training
- Technology
- Information Sharing Techniques and Reporting
- Policy and Requirements

These focal points became the sections under the larger subject areas of the agenda. After the data collection phase was complete, the structure of the TTX took form. The TTX had two goals:

1. Fulfill the recommendations and requirements of the Fort Hood Recommendations & Behavioral Analysis Study for the Force Protection/Physical Security community
2. Ensure the Force Protection/Physical Security community's requirements to detect, deter, and report insider threats of disgruntled, disillusioned, or radicalized individuals who threaten personnel and resources are being addressed...and if not, develop a way ahead accordingly

As the Findings and Recommendations from the Fort Hood Independent Review were progressing, the level of effort to mitigate the insider threat was gaining momentum not only across the DoD, other USG organizations, Academia, and SMEs. It became apparent that communities and stakeholders outside of the Force Protection/Physical Security community could also greatly benefit from the sharing of the information generated by the TTX.

5.3 Results

The TTX was a three day event attended by more than 115 individuals from over 70 different organizations. Each day addressed the sections (listed above) by larger subject areas:

Day 1: Overview and Situational Awareness

Day 2: Training and Technology

Day 3: Information Sharing, Policy, and Requirements

The briefings were provided by key personnel and organizations from the DoD, other USG Organizations, Academia, and SMEs. At the conclusion of each section, a discussion period took

place to identify what (if any) gaps existed in that subject area, and any duplicative efforts that could collaborate or team together to potentially offer a cost-savings benefit, or a “more joint” solution. The group was asked to provide their recommendations to address anything identified. Overall, there were 11 recommendations from the TTX, which are discussed in more detail in Section 5 of this report:

1. Need to produce a Terms of Reference to foster a common insider threat vernacular.
2. DoD needs to do due-diligence in regards to “indicators.” Reviewing the current published indicators and completing a “scientific study” that was tasked to the Defense Science Board (DSB).
3. Reporting requirements (too include online) needs to be better defined and incorporated into training modules across the DoD.
4. Recommend that the Service representatives who are responsible for their Service's insider threat training confirm they have no further requirements or modifications with their training solutions at the next Insider Threat Working Group.
5. Explore adopting/adapting the Transportation Security Administration’s (TSA) Screening Passengers by Observation Techniques (SPOT) training for DoD Application.
6. Army and Air Force should work with the Naval Criminal Investigative Service (NCIS) to leverage the lessons learned and success achieved with their Threat Management Unit (TMU).
7. Potential of a technology demonstration for Visitor Centers or secondary screening of the sensor technologies discussed at the TTX.
8. Need another TTX to continue collaboration amongst the USG, Academia, and SMEs.
9. Need to conduct a study to address the gaps identified during the TTX.
10. Review feasibility of putting all data at the Defense Manpower Data Center (DMDC) and the need for an Office of Primary Responsibility (OPR) for continuous evaluation policy.
11. The DoD needs to ensure that all deployable solutions (including training) for an insider threat, provide military leaders (supervisors, commanders, etc.) “with the tools and discretion they need to take appropriate action to prevent and respond to potential problems.” Information sharing, access to personnel records, and risk assessment (systems) were listed as immediate focus areas.

The After Action Report (AAR) was released which summarized the information that was generated during the discussion sessions at the TTX, with key “take aways” from each day and the recommendations listed above.

6. INTEGRATED WATERSIDE SECURITY

6.1 Background

Navy vessels while docked pier side depend on the security posture of the DoD installation or host nation port security organization to protect it from surface, subsurface, air and landward threats, both conventional and asymmetric. Since the early 1990's the Navy has provided funding for development of waterside security systems to enhance the protection of Navy vessels while in port whether that location be in homeport or an overseas port provided by a host nation. Concerns about the security of vessels in port long preceded the attack on USS COLE (DDG-76) in October 2000. In the intervening years the PSEAG and Navy/Marine Corps have continued to provide funding for further development of systems and security forces to enhance the force protection posture of Navy vessels pier side in order to detect and engage surface and subsurface threats at some stand-off distance. Challenges in the development of force protection systems at waterfront facilities have included the fielding of systems that are large, marginally effective, difficult and expensive to maintain, and manpower intensive. New systems are needed with a more common interface such that an average skilled Sailor with basic system training can operate the system effectively with confidence. At the same time the fielded systems must be cost effective to maintain and to upgrade over the lifecycle of the system. While there are systems, weapons and security personnel focused on providing waterside security, what is not well developed are the means and methods for the Navy vessel pier side or at anchor to maintain situational awareness (SA) of changes to the security environment in the port and the surrounding environs. The gap appears to be a truly Integrated Waterside Security System that optimizes the available manpower and systems of Navy/Marine Corps security assets ashore and afloat in order to protect critical infrastructure ashore and High Value Units (HVUs) pierside from natural and man-made disasters, terrorist attack or conventional attack through the various levels of FPCON.

6.2 Purpose and Goals

Phase I of the Department of the Navy, Integrated Waterside Security study collected data and information from a representative sampling of naval stations, naval air stations, naval weapons stations, and submarine bases, all with waterside security issues, along with information collected from their parent Regional Security Officers/Force Protection Program Directors. Site visits to these various naval installations included meetings with commanding officers of ships, AT/Physical Security Officers at the region and installation commanding officers to discuss the major issues that impact physical security/force protection readiness including policies, procedures, personnel/manpower and systems (command and control, sensors, cameras, port security barriers (PSBs), Harbor Security Boats (HSBs), and weapons, both gun systems and NLWs). Analysis of information collected indicated both organizational gaps as well as systems capability gaps impact the level of effectiveness for installation security on the waterfront. The following were Phase I accomplishments:

- Reviewed current Navy/Marine Corps planning, funding and R&D activities directed to waterside security system developments.
- Reviewed documentation related to waterside security development efforts and performance of existing legacy systems.

- Identified strengths and weaknesses of existing legacy systems both at the system level and the organizational integration level.
- Identified organizational level weaknesses in the optimization of these systems across the ship/shore integration line (at the pier).
- Interviewed key Navy and Marine Corps headquarters and Support Agencies to develop positions/alternatives/options that might be pursued in developing a revised Navy Approach to the security interface between Navy vessels docked pier side and the security organization ashore.

Phase II of the Integrated Waterside Security study utilized the information collected in Phase I to develop a process for an Analysis of Alternatives (AoA) approach to find what systems improvements will likely lead to the greatest improvements in Force Protection/Physical Security readiness for the Afloat-Ashore Integration Initiative inherent to an Integrated Waterside Security framework. The following were Phase II accomplishments:

- Prepared for and facilitate a Navy/Marine Corps waterside security conference and presented findings of gaps at the organizational and systems level across the ship/shore integration line (at the pier). Reviewed gaps and evaluated possible alternatives and selected the preferred alternative.
- Developed a matrix of waterside security capability elements to include the element status, funding profile and ongoing RDTE work associated with still developing technologies for new systems.
- Conducted an Analysis of Alternatives using the expertise of key waterside security stakeholders that will identify new approaches and systems that will enhance waterside security.

Phase III of the Navy, Integrated Waterside Security study is further developing the prioritized list of R&D focus areas for use in planning an Integrated Waterside Security Concept Demonstration that will incorporate a number of new technologies in to a test demonstration. New approaches to force protection, that increase communications and situational awareness across the waterfront, while optimizing available manpower and systems of Navy/Marine Corps assets ashore and afloat in order to protect Navy vessels, critical infrastructure ashore and HVUs pier side from terrorist and asymmetric attacks (through the various levels of FPCON) need to be explored through further research and development efforts, particularly for improved effectiveness in FPCON Alpha and Bravo. Phase III of the Integrated Waterside Security study will utilize the information collected in Phase I and the Analysis of Alternatives (AoA) developed in Phase II to identify a set of advanced technologies that will be integrated in to a concept demonstration to test and evaluate which systems will likely lead to the greatest improvements in Force Protection/Physical Security effectiveness.